BILLING CODE 7710-12

POSTAL SERVICE

Privacy Act of 1974; System of Records

AGENCY: Postal Service™.

ACTION: Notice of a modified system of records.

SUMMARY: The United States Postal Service™ (USPS™) is proposing to modify a General Privacy Act System of Records to support the implementation of a suite of cloud-based workplace productivity software.

DATES: These revisions will become effective without further notice on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, unless comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be submitted via email to the Privacy and Records Management Office, United States Postal Service Headquarters (privacy@usps.gov). Arrangements to view copies of any written comments received, to facilitate public inspection, will be made upon request.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or privacy@usps.gov.

SUPPLEMENTARY INFORMATION: This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the Federal Register when there is a revision, change, or addition, or when the agency establishes a new system of records.

I. Background

The Postal Service is constantly seeking methods to improve employee productivity and efficiency. To that end, the Postal Service will implement a suite of cloud-based workplace productivity applications. These applications will expand employee access to various programs, allowing more employees to utilize resources to increase productivity and team collaboration.

II. Rationale for Changes to USPS Privacy Act Systems of Records

The Postal Service is proposing to modify USPS System of Records (SOR) 550.000 Commercial Information Technology Resources- Infrastructure to support the implementation of a suite of cloud-based workplace productivity software. This system will be modified in conjunction with USPS 550.100 Commercial Information Technology Resources- Applications and USPS 550.200 Commercial Information Technology Resources- Administrative to reflect the full scope of application implementation. Revisions to these SORs will be submitted independent of this notice. More information on accompanying changes can be found within those SORs.

This system specifically reflects data elements collected, gathered, or used to provide application access generally. Revisions to the existing SOR to support this implementation are documented as additions to existing categories of records *Information System Account Access records* beginning with “Last Sign-In Time” and *Security Analytics records* beginning with “Login IP Address.”

III. Description of the Modified System of Records

Pursuant to 5 U.S.C. 552a (e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed revisions has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect this amended system of records to have any adverse effect on individual privacy rights. The notice for USPS 550.000

Commercial Information Technology Resources- Infrastructure, provided below in its entirety, is as follows:

SYSTEM NAME AND NUMBER: 550.000 Commercial Information Technology Resources- Infrastructure

SECURITY CLASSIFICATION: None.

SYSTEM LOCATION: All USPS facilities and contractor sites.

SYSTEM MANAGER(S): For records of computer access authorizations: Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 39 U.S.C. 401, 403, and 404.

PURPOSE(S) OF THE SYSTEM:

1. To provide USPS employees, contractors, and other authorized individuals with hierarchical access to and accounts for commercial information technology resources administered by the Postal Service and based on least privileged access.
2. To facilitate a cohesive software experience and simplify ease of use by sharing user and application data across participating IT programs.
3. To authenticate user identity for the purpose of accessing USPS information systems.
4. To assess user attributes and assign related access privileges.
5. To authenticate suppliers and contractors and facilitate further access to downstream Postal Service information systems.
6. To provide active and passive monitoring of information systems, applications, software, devices, and users for information security risks.
7. To review information systems, applications, software, devices, and users to ensure compliance with USPS regulations.
8. To facilitate and support cybersecurity investigations of detected or reported information security incidents.

9. To administer programs, processes, and procedures to assess information security risks and to detect information security threats and vulnerabilities.
10. To provide tools and analytics for USPS employees and contractors to measure work productivity and improve efficiency.
11. To improve manager-subordinate relationships within their formal reporting structure through data-based insights generated from their own email and related electronic communications with subordinates.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Individuals with authorized access to USPS computers, information resources, and facilities, including employees, contractors, business partners, suppliers, and third parties.
2. Individuals participating in web-based meetings, web-based video conferencing, web-based communication applications, and web-based collaboration applications.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. *Information System Account Access records*: Records relating to the access or use of an information system, application, or piece of software, including; Name, User ID, Email Address, User Type, User Role, Job Title, Department, Manager, Company, Street Address, State Or Province, Country Or Region, Work Phone Number(S), Employee Identification Number (EIN), Advanced Computing Environment (ACE) ID, License Information, Action Initiated, Datetime, User Principle Name, Usage Location, Alternate Email Address, Proxy Address, Age Group**,** IP Address, MAC Address, Password, Multi-Factor Authentication Credentials, Security Questions, Security Answers, Passcode, Geolocation Data, User Profile Picture, Picture Metadata, Information Technology Account Administration User Configuration Status, Supplier Credentials, Supplier Company Codes, Conditional Access Attributes, Last Sign-In Time, User Account Status, User Admin Status, Password

Length Compliance, Password Strength, Number Of Installed External Apps, Less Secure Apps Access, Admin-Defined Name, Profile Name Status, Photo Storage Space Used, Total Storage Space Used, Storage Usage Percentage, Total Emails Sent, Total Emails Received, Total Emails Sent And Received, Email Server Last Usage Time, Device Application Change, Device Privilege Changed, Device Policy Changed, Device Action Reported, Device Compliance Status, Device Operating System Updated, Device Ownership Updated, Device Settings Changed, Device Status Changed Through Apple Device Enrollment, Device Account Synced, Device Risk Signal Updated, Device Work Profile Submitted.

2. *Security Analytics records*: Records relating to the gathering, analysis, review, monitoring, and investigation of information system security risks, including; User Investigation Priority Score, User Identity Risk Level, User Lateral Movement Paths, User Devices Numbers, User Account Numbers, User Resources Numbers, User Locations Numbers, User Matches Files Numbers, User Locations , Apps Used By User, User Groups, User Last Seen Date, User Affiliation, User Domain, App Instance, Organizational Groups, User Account Status, Activity ID, Activity Objects, Activity Type, Administrative Activity, Alert ID, Applied Action, Activity Date, Device Tag, Activity Files And Folders, Impersonated Activities, App Instance Activity, App Location Activity, Activity Matched Policy, Activity Registered ISP, Activity Source, Activity User, Activity User Agent, Activity User Agent Tag, Application Risk Score, Application Activity, User Software Deactivation, User Software Installation, User Software Removal, Last Date Of Software Execution, Internet Application Transaction Counts, Data Volume Upload, Data Volume Download, Data Sensitivity Classification, Internet Protocol, Internet Port, And Internet Access History, Login IP Address, Login Type, Login Failed, Login Successful, Number Of Times A User Was Suspended, Number Of Times A User Was Suspended Due To Spam Relay,

Number Of Times A User Was Suspended Due To Spam, Number Of Times A User Was Suspended Due To Suspicious Activity, Device Name, Device Operating System, Days Since First Sync, Days Since Last Sync, Device Status, Device Type, Device Model, Device Account Registration Changed, Device Action Event, Device Compliance Status, Device Compromise Status, Device Ownership Change, Device Operating System Updated, Device Settings Changed, Device Failed Screen Unlock Attempts, Device Status Changed On Apple Portal, Device User Signed Out, Device Suspicious Activity Detected, Device Work Profile Supported, Two-Factor Authentication Disabled, Two-Factor Authentication Enrolled, Account Password Changed, Account Recovery Email Changed, Account Recovery Phone Number Changed, Account Recovery Secret Question Changed, Account Recovery Secret Answer Changed, Account Password Leak Suspected, Account Suspicious Login Blocked, Account Suspicious Login From Less Secure App Blocked, Suspicious Programmatic Login Blocked, User Suspended, User Suspended (Spam Through Relay), User Suspended (Spam), User Suspended (Suspicious Activity), Account Enrolled In Advanced Protection, Account Unenrolled In Advanced Protection, Account Targeted By Government-Backed Attack, Out Of Domain Email Forwarding Enabled, Login Challenge Question Presented, Login Verification Presented, Log Out, Secure Shell Public Key Added, Secure Shell Public Key Deleted, Secure Shell Public Key Retrieved, Secure Shell Public Key Updated, Login Profile Retrieved, POSIX Account Deleted, Application Method Called, Application Access Authorized, Application Access Revoked, Device Compromised, Failed Password Attempts On User Device, Device Property Changed.

3. *Productivity Analytics records*: Records relating to the gathering, analysis, review, and investigation of information system utilization, including; Calendar Appointments, Email Read Rate, Email Response Rate, Operating System Activity History, Email

Timestamp, Statements Made In Email Body, Email Sender, Email Recipient, Email Subject Line, Calendar Event Type, Calendar Event Status, Calendar Event Category, Calendar Event Subject, Calendar Event Duration, Calendar Event Attendees, Meeting Organizer, Meeting Invitees, Meeting Subject Line, Meeting Scheduled Time, Meeting Attendee Status, Meeting Scheduled Location, Web Call Organizer, Web Call Invitees, Web Call Scheduled Time, Web Call Joined Time, Web Call Duration, Web Call Status, Web Call Join Status, Number Of Collaborative Audio Calls Made, Number Of Collaborative Video Calls Made, Chat Initiator, Chat Recipient, Chat IM Sent Time, Number Of Cloud-Based Personal Storage Documents Worked On, Number Of Cloud-Based Enterprise Storage Documents Worked On, Device Name.

RECORD SOURCE CATEGORIES: Employees; contractors; customers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES

OF USERS AND THE PURPOSES OF SUCH USES: Standard routine uses 1. through 9. apply. In addition:

a) To appropriate agencies, entities, and persons when (1) the Postal Service suspects or has confirmed that there has been a breach of the system of records; (2) the Postal Service has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Postal Service (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Postal Service's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Automated database, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

1. Records relating to information system access are retrievable by name, email address, username, geolocation data, and ACE ID.
2. Records relating to security analysis are retrievable by name, unique user ID, email address, geolocation data, IP address and computer name.
3. Records relating to productivity are retrievable by name, email address, and ACE ID.
4. Records relating to third-parties are retrievable by name, email address, user name, and IP address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Records relating to information system access are retained twenty-four months after last access.
2. Records relating to security analysis are retained for twenty-four months.
3. Records relating to productivity are retained for twenty-four months.
4. Records relating to third-parties are retained for twenty-four months.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Computer access is limited to authorized personnel with a current security clearance, and physical access is limited to authorized personnel who must be identified with a badge.

Access to records is limited to individuals whose official duties require such access. Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections.

Computers are protected by encryption, mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls

including access controls, terminal and transaction logging, and file management software.

RECORD ACCESS PROCEDURES: Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES: See Notification Procedure and Record Access Procedures above.

NOTIFICATION PROCEDURES: Customers wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the Chief Information Officer and Executive Vice President and include their name and address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: May 10th, 2021; 86 FR 24907.

* * * * *

Joshua J. Hofer,

Attorney, Ethics and Legal Compliance.

[FR Doc. 2022-01062 Filed: 1/28/2022 8:45 am; Publication Date: 1/31/2022]